

Fig. 1
PRIOR ART

FIG. 2 is a block diagram of a digital signature verification process 200. The process 200 receives a message 110 and a digital signature 180 from a signer 190. The message 110 is input to a hash function 120, which produces a hash result 220. The digital signature 180 and the hash result 220 are input to a verify function 240. The verify function 240 also receives a public key 260. The verify function 240 outputs a valid? result 280.

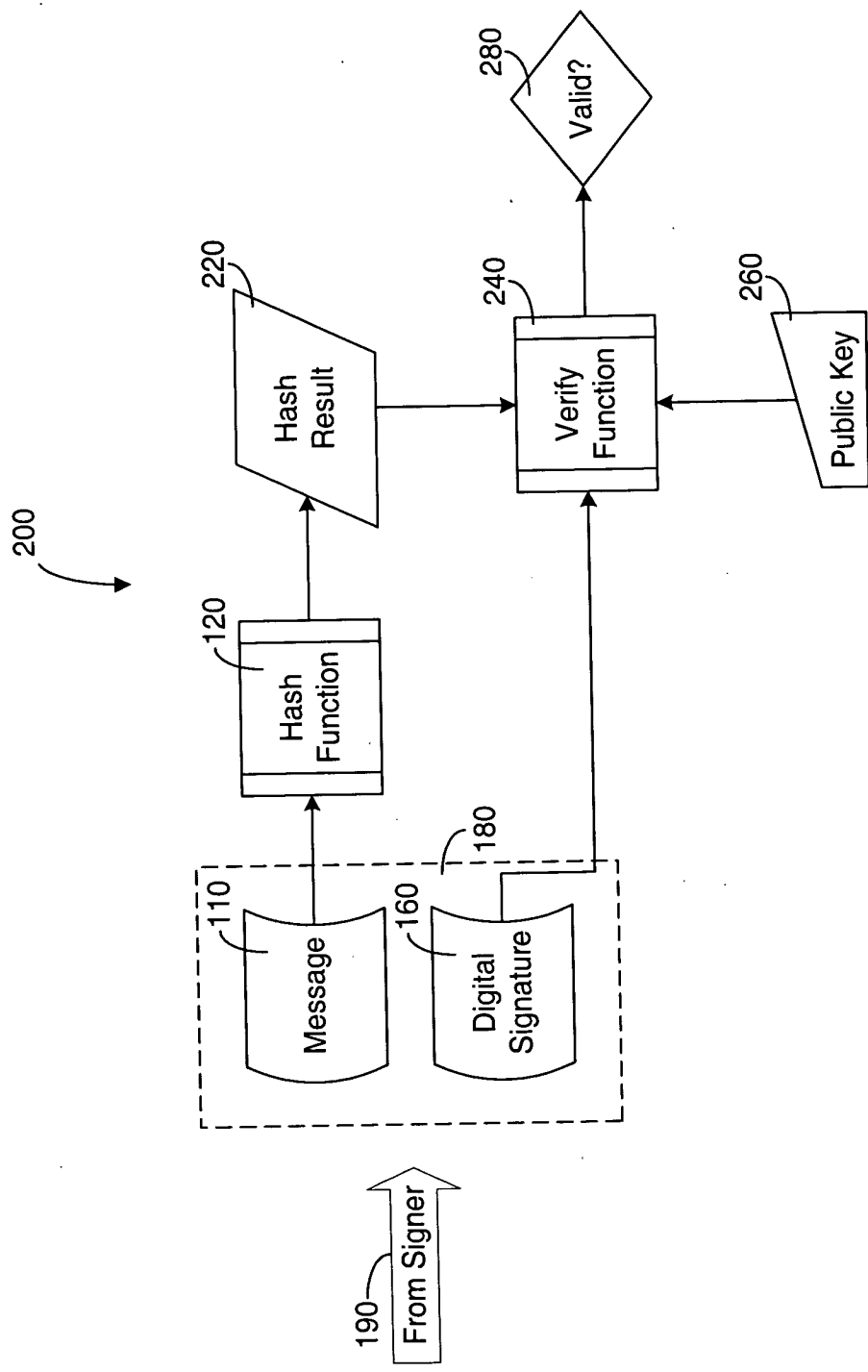


Fig. 2
PRIOR ART

FIG. 3 is a block diagram of a system 300 for secure data storage and retrieval. The system 300 includes a data source 305, a data storage device 310, a data retrieval device 315, a data processing unit 320, a data encryption/decryption unit 325, a data key management unit 330, a data key storage unit 335, a data key retrieval unit 340, a data key distribution unit 345, a data key storage unit 350, a data key retrieval unit 355, a data key distribution unit 360, a data key storage unit 365, a data key retrieval unit 370, and a data key distribution unit 375.

300

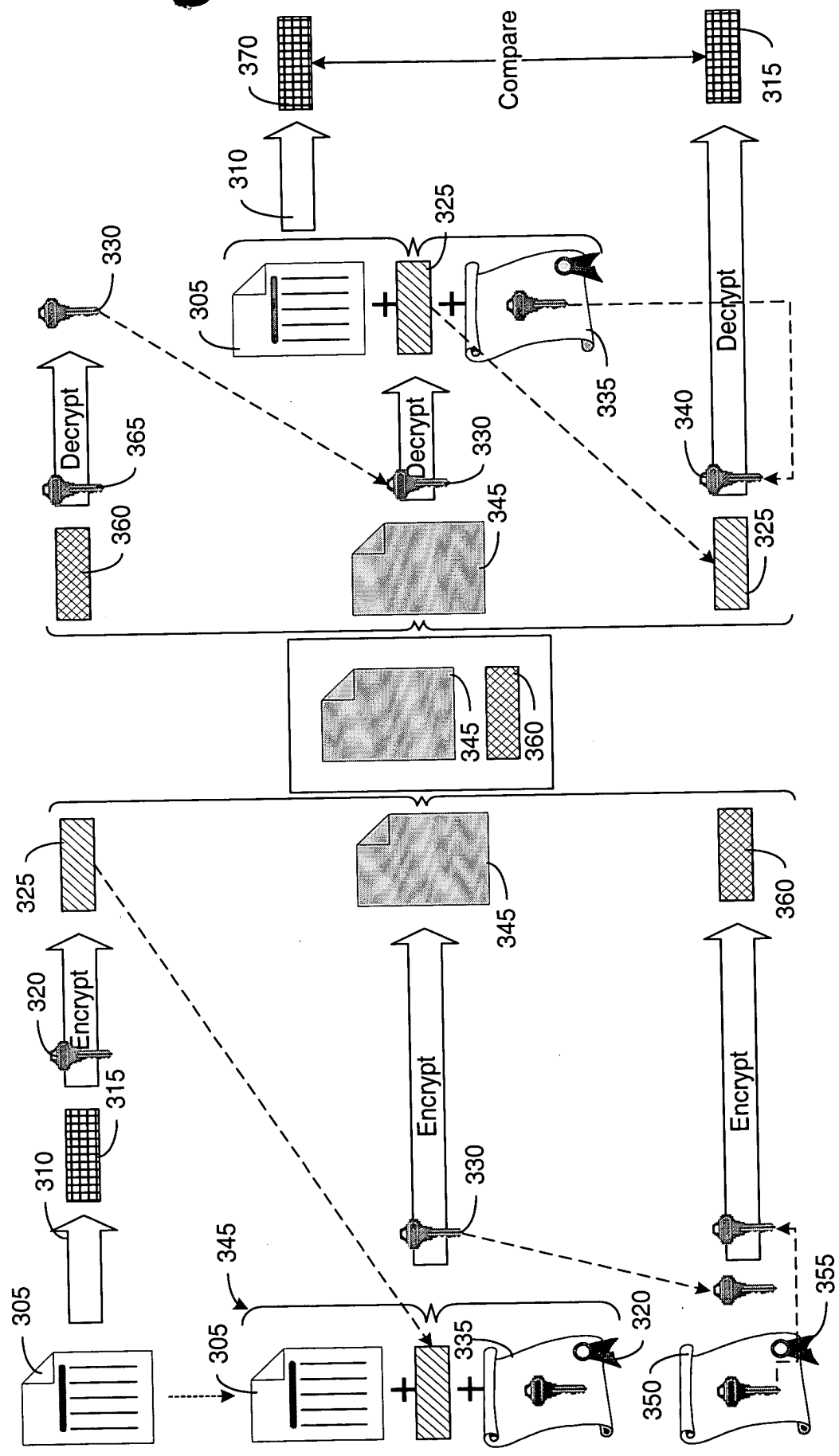


Fig. 3
Prior Art

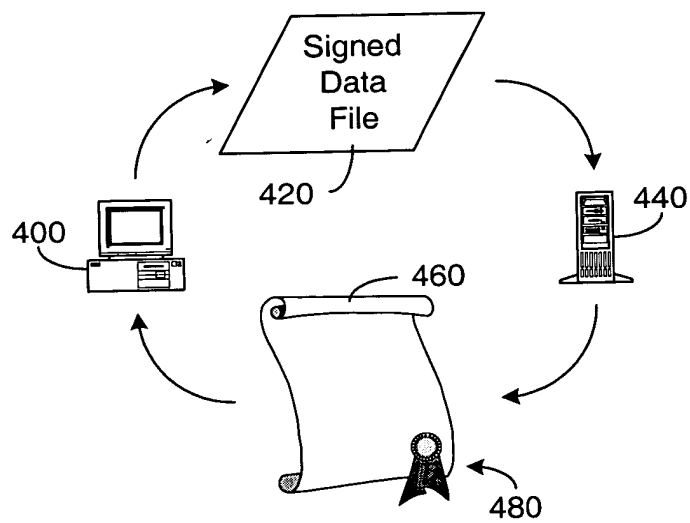


Fig. 4
PRIOR ART

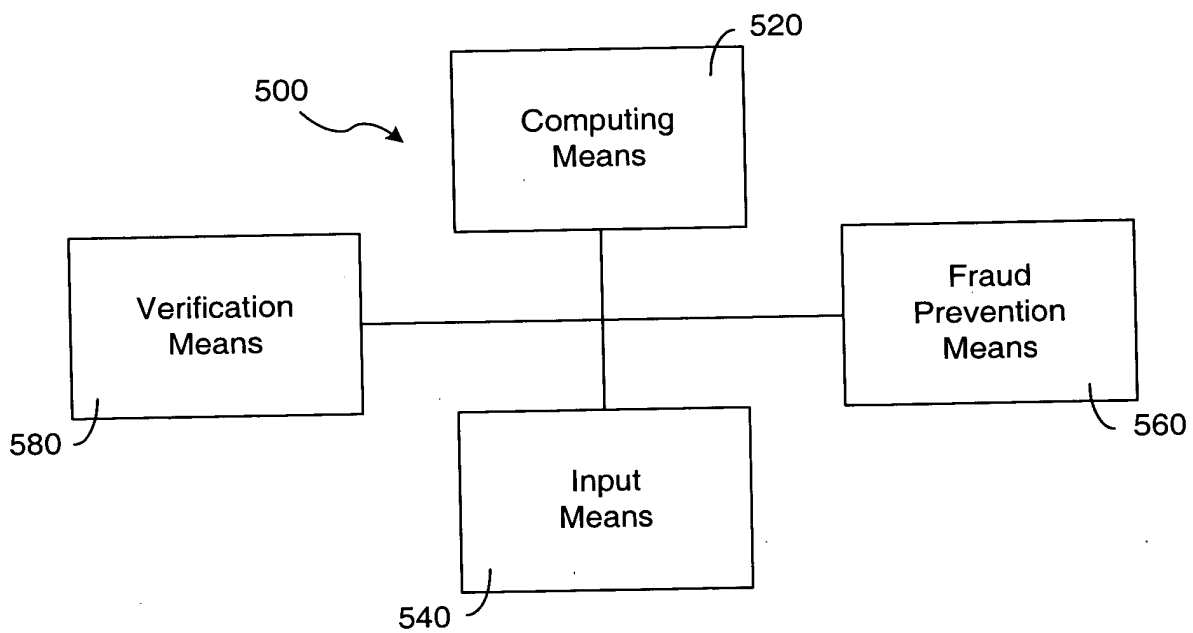


Fig. 5

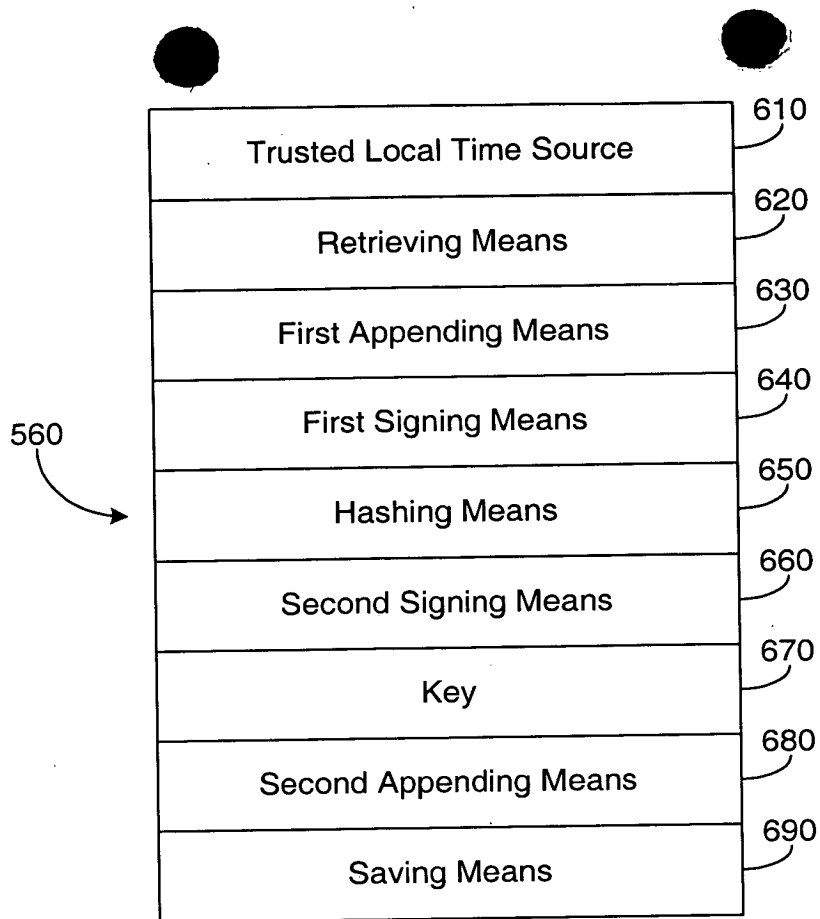


Fig. 6

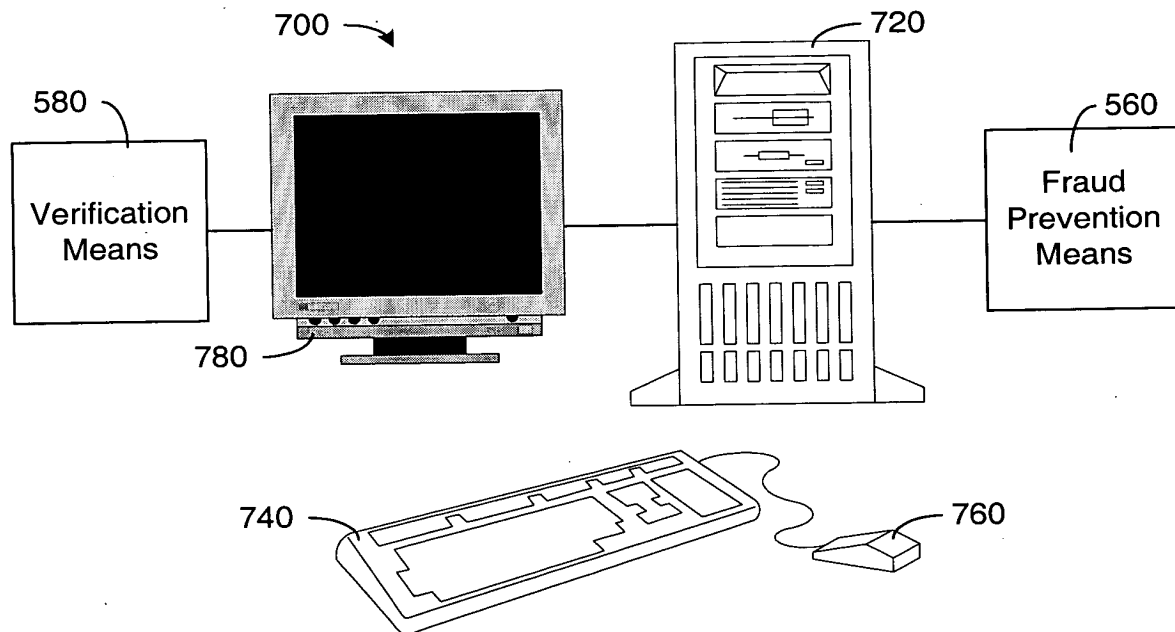


Fig. 7

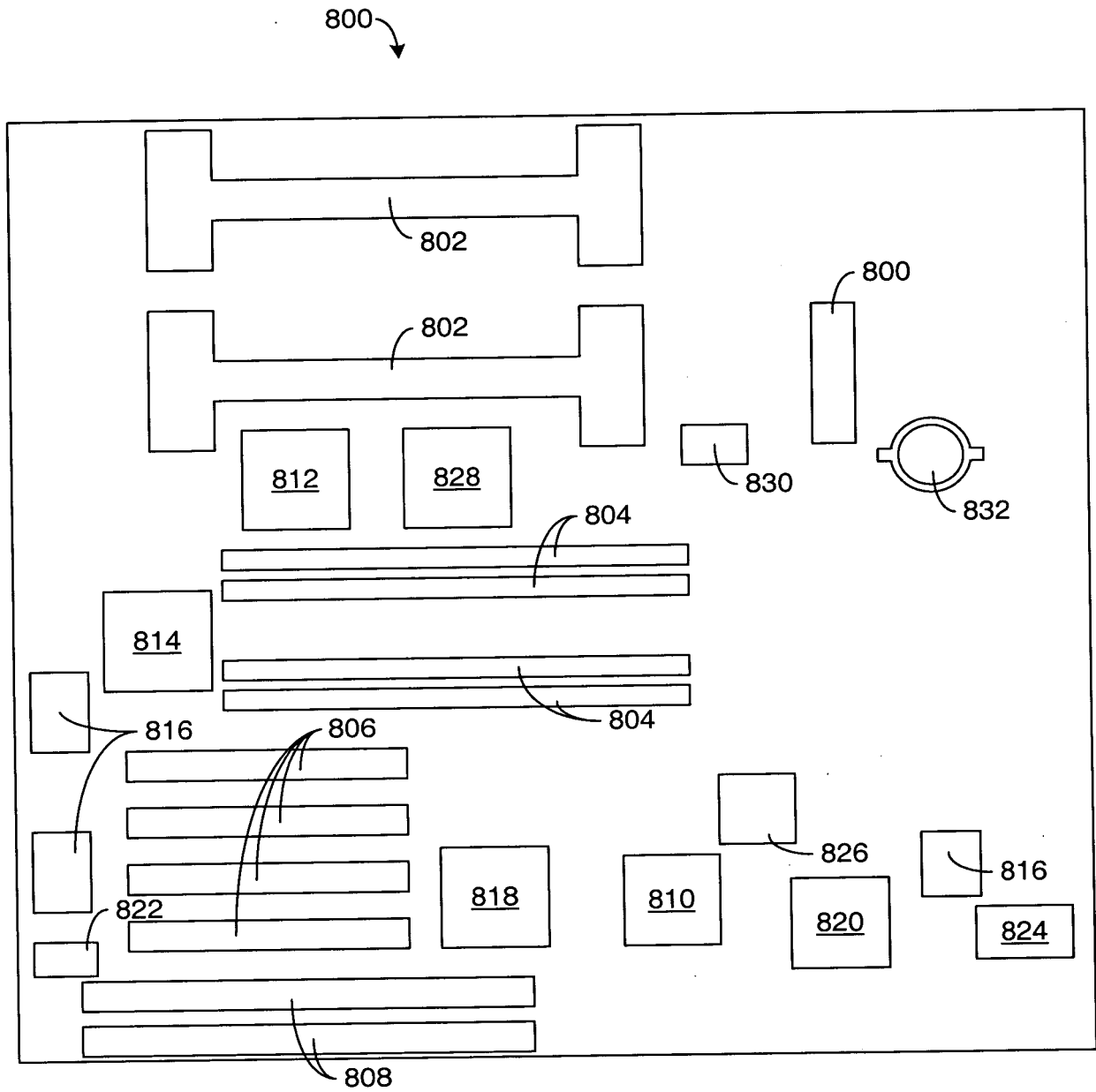


Fig. 8

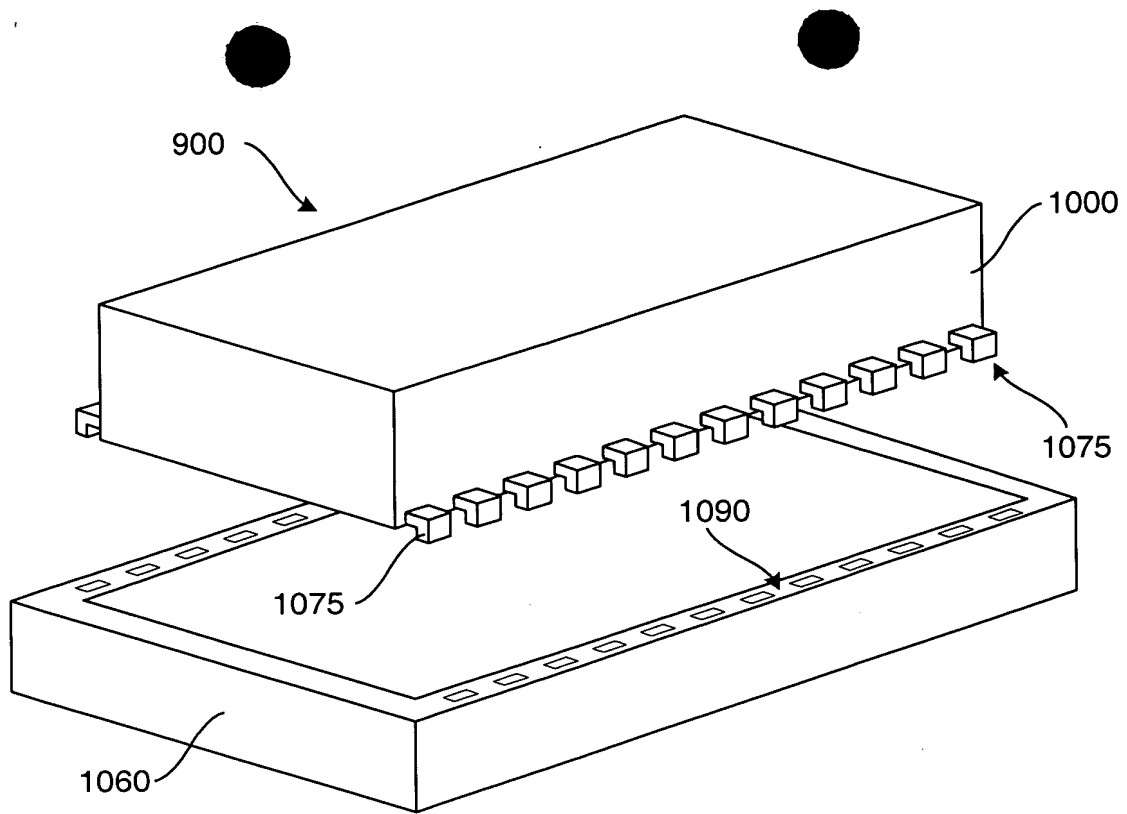


Fig. 9

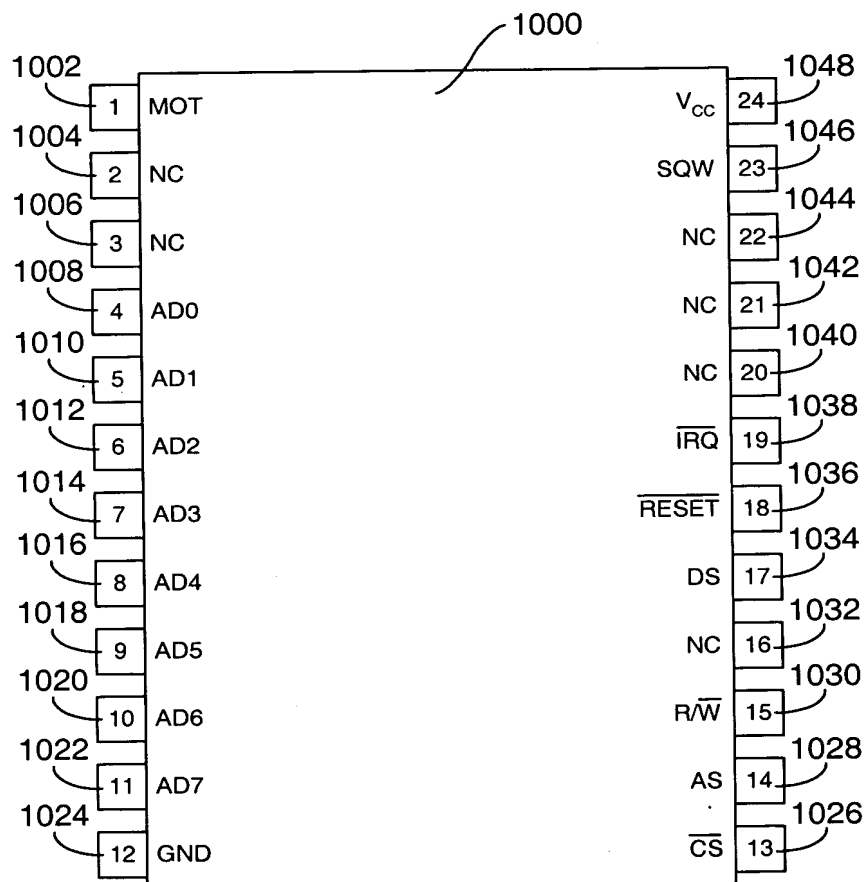


Fig. 10

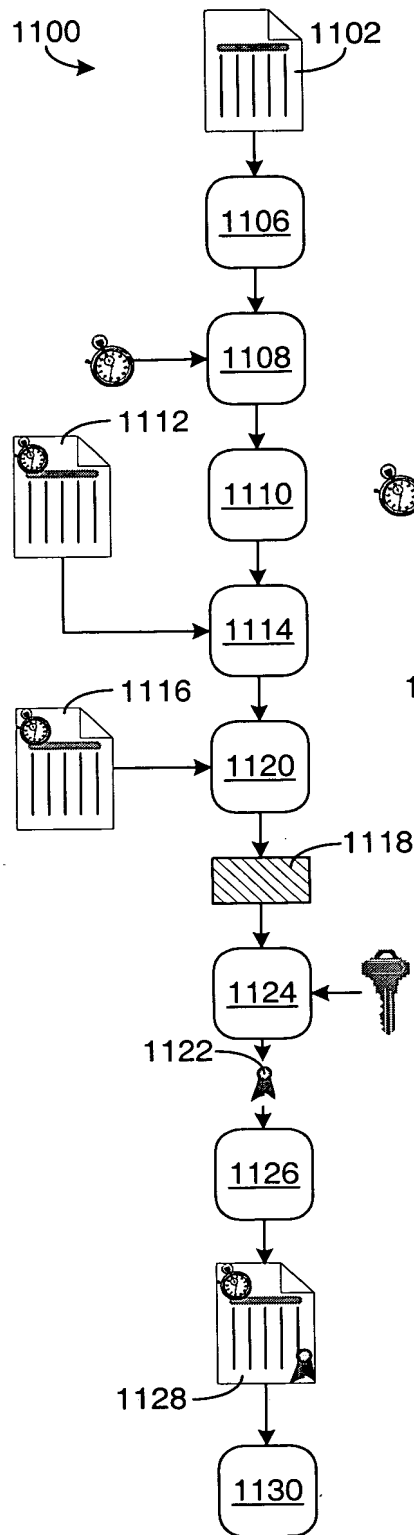


Fig. 11(a)

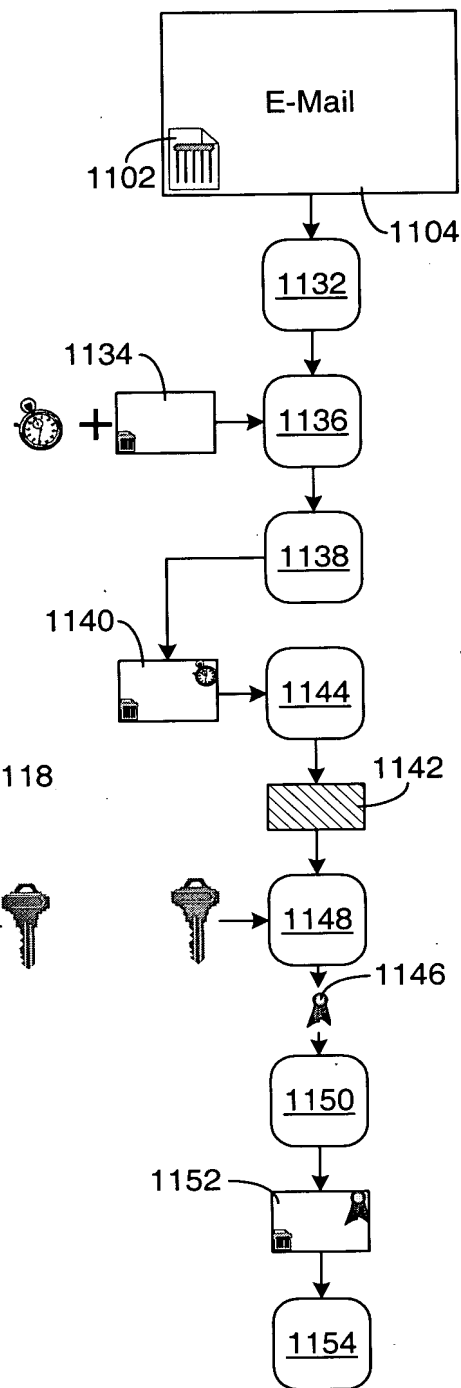


Fig. 11(b)

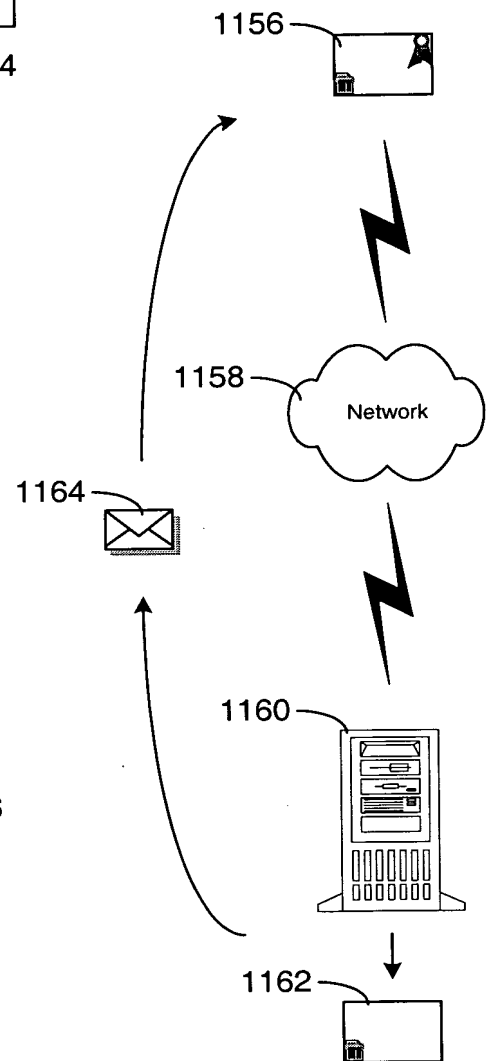


Fig. 11(c)

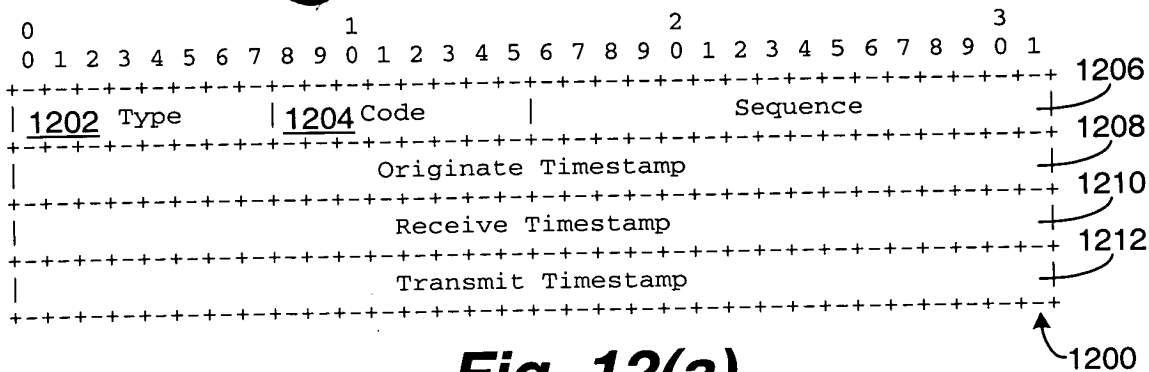


Fig. 12(a)

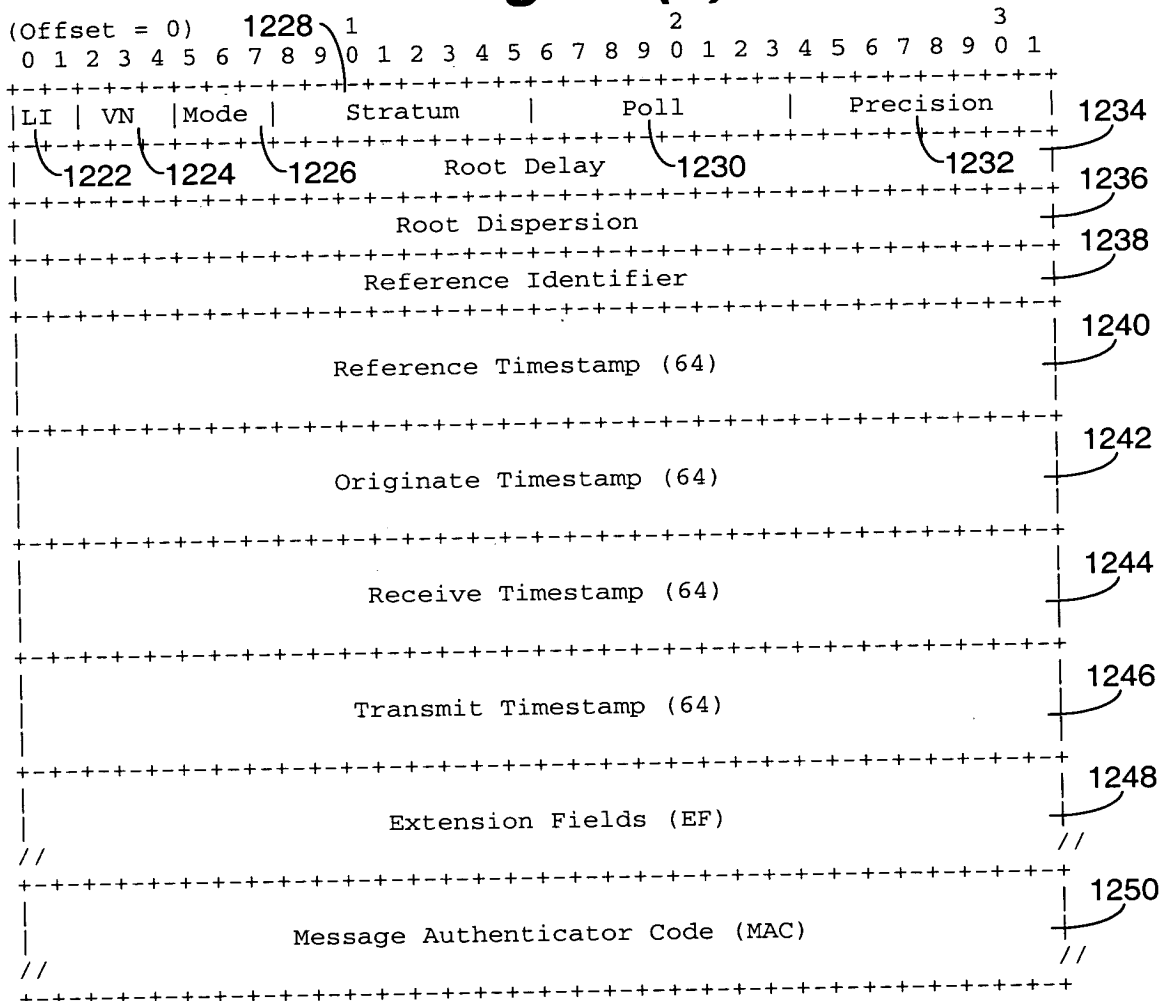


Fig. 12(b)

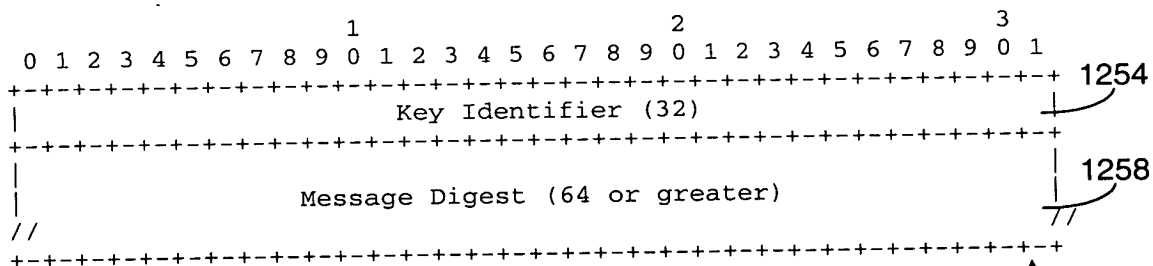


Fig. 12(c)

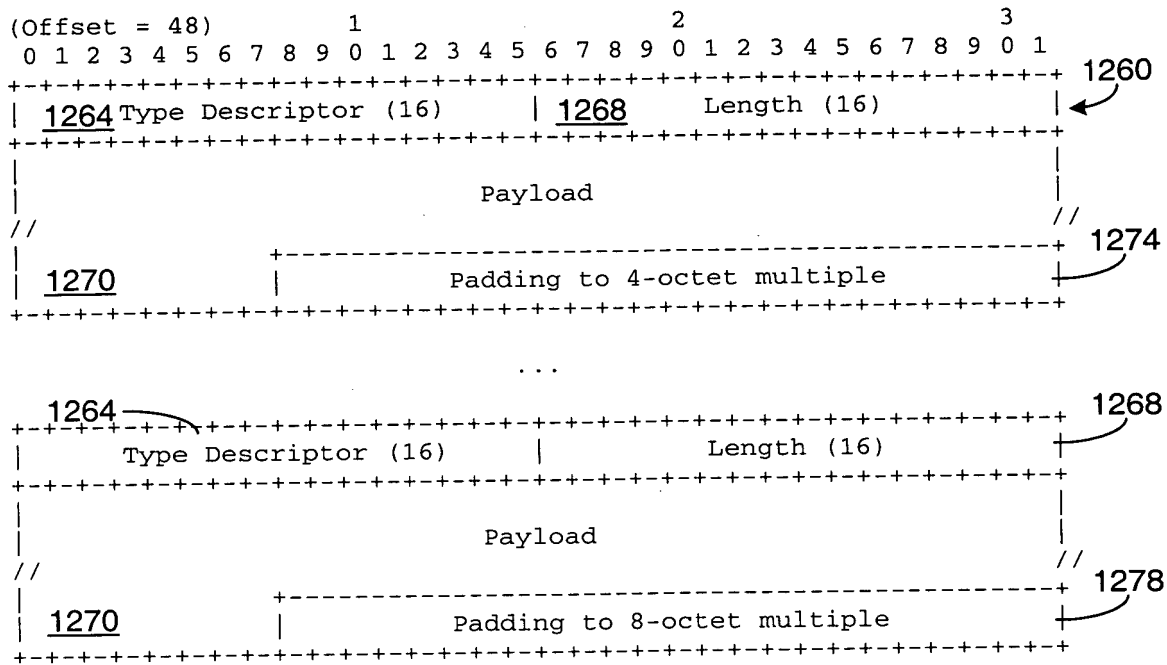


Fig. 12(d)